Commonwealth of Massachusetts
Executive Office of Technology Services and Security (EOTSS)
Enterprise Security Office

Glossary of Terms

Document Name: Glossary of Terms	Effective Date: October 15, 2018
Document ID: IS.Glossary	Last Revised Date: November 04, 2021

Table of contents

1. PURPOSE

The purpose of this ***standard*** is to provide a centralized, common reference for definitions of terms used in information security ***policies*** and ***standards***.

2. SCOPE

This document applies to the use of information, information systems, electronic and computing devices, applications, and network resources used to conduct business on behalf of the Commonwealth. The document applies to the Executive Department including all executive offices, and all boards, commissions, agencies, departments, divisions, councils, and bureaus.. Other Commonwealth entities that voluntarily use or participate in services provided by the Executive Office of Technology Services and Security, such as mass.gov, must agree to comply with this document as a condition of use. Executive Department agencies and offices are required to implement procedures that ensure their ***personnel***, including consultants, contractors, and vendors, comply with the requirements herein to safeguard information.

3. RESPONSIBILITY

3.1 The Enterprise Security Office is responsible for the development and ongoing maintenance of this document.

3.2 The Enterprise Security Office is responsible for compliance with this document and may enlist other departments to assist in monitoring and maintaining compliance.

3.3 Any inquiries or comments regarding this document shall be submitted to the Enterprise Security Office by sending an email EOTSS-DL-Security Office.

3.4 Additional information regarding this document may be found at https://www.mass.gov/cybersecurity/policies.

4. DEFINITIONS

Access Control – Specific implementation or configuration intending to (fully or partially) mitigate a risk related to unauthorized parties accessing the Commonwealth's assets.
Administrative Account (Privileged Account) – An information system account where a user is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Asset – Any entity that the Commonwealth considers to have value. Assets can be tangible (e.g., computers, mobiles, network equipment and media) or intangible (information-related – e.g., information, software and services). The Commonwealth considers information as an asset.

Business Recovery Event – Unplanned outage where the Recovery Time Objective is in jeopardy.

Cloud Computing – Cloud computing is an approach to computing infrastructure typically defined by on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. Deployments are subscription-based and delivered over the internet via an "as-a-service" model and can scale to meet the changing demands of the business. Cloud deployments could be Software as a Service, Platform as a Service or Infrastructure as a Service. Cloud Computing may be developed internally, outsourced externally, or implemented through a hybrid model of internal and external methods.

Confidential Information – This is one of four classifications of Information. Specifically, Confidential Information is important to the ongoing operations of the Commonwealth. This Information is primarily used in day-to-day operations. This type of information is for select groups and not available to the general public. Confidential information, if necessary, will be assessed for release under the Massachusetts Public Records Law, and in response to subpoenas and requests for production in litigation, and, subject to any applicable law, will be reviewed under all relevant procedures as to its releasability.

Contractor/Consultant – Personnel directly hired by a firm other than the Commonwealth, accessing the Commonwealth's resources and assets, to support a business agreement or contract with the Commonwealth.

Control – Specific implementation or configuration intending to (fully or partially) mitigate a risk. Controls are embedded into standards and procedures as a means of ensuring accountability and audibility of a process.

Control Owner - An individual who is responsible for the effectiveness of controls within the Commonwealth's information technology (IT) environment.

Crypto Period – A crypto period is the time span during which a specific key is authorized for use by the Commonwealth or the keys for a given system will remain in effect.

Disposal – Removal or destruction of sensitive data/Assets via secure methodology.

ePolicy Orchestrator (ePO) – An extensible and scalable centralized security management software that unifies security management through an open platform and simplifies risk and compliance management for organizations.

Endpoint – Includes desktops, laptops, tablets, smartphones and other mobile devices used to store, process or transmit the Commonwealth's Information.

Equipment – Refers to any tangible device that is used in operation of the Commonwealth business. All equipment are assets; however, not all assets are equipment. Event – Any observable occurrence deemed noteworthy or unusual, as it does not conform to the standard or expected operating behavior.

Governance Risk and Compliance Team - Entity responsible for the management and execution of the risk assessment process as well as approvals and tracking of identified risk mitigations.

High-Value Asset – An asset (e.g. a server, information) that, if it were compromised, would negatively impact the Commonwealth's investment in the asset and threaten the Commonwealth's ability to serve the public.

Impact - The extent to which a risk (if realized) would impact the organization.

Incident – Any event or set of events that creates a potential threat for loss or disruption to business operations, reputation or assets.

Information Asset - Any written business or customer information related to the Commonwealth, including but not limited to reports, emails, database content, code and unorganized information sets.
Information Custodian – Person responsible for overseeing and implementing the necessary safeguards to protect the information system, at the level classified by the Information Owner (e.g., System Administrator, controlling access to a system component).

Information Owner – Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Information Security Team – Team responsible for the protection of Information and Information Systems from unauthorized access, use, disclosure, disruption, modification or destruction to provide confidentiality, integrity and availability.

Information Security Incident – Any incident that compromises the confidentiality, integrity or availability of Information and creates a potential threat for loss or disruption to business operations, reputation or assets and is also a violation of information security Policies or general security practices.

Information System – A discrete set of technology resources organized for the creation, storage, processing, transmission, use or disposal of Information.

Information Technology Management – Individuals or groups with management responsibilities over the design, operations and maintenance of internal and customer-facing technology infrastructure, systems, and processes.

Information Technology Risk – Probability of occurrence of an event combined with its adverse consequences that would impact Information Systems, Information or operations.

Inherent Risk - The exposure to a risk in the absence of controls.
Intellectual Property Rights – Intangible rights that protect the Commonwealth's or its vendors' copyrightable work, patented technology inventions, trademarks and trade secrets.

Internal Use - Information that has NOT been expressly authorized for public release but that has not been classified as confidential. The disclosure of Internal Use information is unlikely to have a material financial, legal, regulatory or reputational impact on the Commonwealth, its constituents, customers and business partners.

Infrastructure as a Service (IaaS) – Type of Cloud Computing provided that allows the Commonwealth to use a cloud provider's infrastructure for fundamental computing requirements (e.g., storage, hardware or servers).

Key – Data that is used to encrypt or decrypt information using a cryptographic algorithm.

Legal – the Office of General Counsel of Massachusetts Executive Office of Technology Services and Security (unless otherwise explicitly stated in text).

Log – A record of the Events occurring within an organization's systems and networks.

Malware – Consists of a variety of forms of hostile, intrusive or annoying software or program code designed to disrupt operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and cause other abusive behavior. Examples include, but are not limited to, computer viruses, worms, Trojan horses, spyware, adware, and other malicious and unwanted software or programs.

Mobile Device – A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, onboard sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smartphones, tablets, and E-readers (generally running a mobile operating system).

Module – When developing a network architecture, industry leading practice is to break down the larger, more complex enterprise network into smaller manageable areas called modules. These modules are intended to logically categorize network platforms, systems and end-user devices into high-level areas that serve a distinct role and whose unique functions and features collectively constitute effective network architecture.

Originator Usage Period – The period of time during which cryptographic protection may be applied to data is called the originator usage period, and the period of time during which the protected information is processed is called the recipient usage period.

Passphrase – A passphrase is a sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage but is generally longer for added security. Passphrases should have the following characteristics:

- Long enough to be hard to guess
- Not a famous quotation from literature, holy books, et cetera
- Hard to guess by intuition—even by someone who knows the user well
- Easy to remember and type accurately

One method to create a strong passphrase is to use dice to select words at random from a long list. Another method is to choose two phrases, turn one into an acronym and include it in the second, making the final passphrase. Passphrases are preferred over passwords as they are more difficult to crack.

Personnel – The Commonwealth's state employees, contractors, consultants, vendors, and interns, including full-time, part-time, or voluntary.

Policy – Management statement on a topic defining the direction of the organization and describing the cultural norms and values to be upheld.
Procedure – Technical documentation describing specific steps to configure systems or perform tasks in a manner which supports the related standard and Policies.

Process Owner - An individual who is responsible for the management and operations of identified IT processes.

Public - Information that has been expressly approved for public release.

Remote Access – Any access to internal Commonwealth information assets from any external non-Commonwealth location, including Mobile-Access VPN and Site-to-Site Remote Access.

Residual Risk - Risk level that exists taking into consideration the treatment of risks utilizing controls.

Risk - A risk is any event or circumstance that could adversely affect the achievement of organizational objectives. Risk is defined in terms of the likelihood of occurrence and impact if it occurs.

Risk Governance Committee - Committee responsible for the oversight of the risk assessment process.

Risk Tolerance - The willingness of an organization to accept a given level of risk. Clarifying risk tolerance levels supports informed decision-making by assisting in identifying the level of risk that is permissible.
Security Administrator – Personnel with security administration roles that are responsible for the creation of accounts and the assignment of privileges.

Security Incident Response Team (SIRT) – a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity.

Standard – Management statement describing the behavioral expectations or technical implementations of the related sub-Policies and Policies.

Stateful Traffic Inspection – The inspection of traffic by platforms and systems where the state of connections is monitored for non-compliance with information in a state table.

Third Parties – Third Parties are individuals or firms that are not the Commonwealth's employees or the Commonwealth's entities, but that have access to the Commonwealth's resources.

Two-Factor Authentication: Authentication using two of the following:

- Something you know (i.e., a password)
- Something you have (i.e., a token device or smart card)
- Something you are (i.e., biometrics—fingerprint, retinal scan, etc.)

User – A person or entity (e.g., system, service) with authorized access.

5. DOCUMENT CHANGE CONTROL

Version No.	Revised by	Effective date	Description of changes
0.90	Jim Cusson	10/01/2017	Corrections and formatting.
0.95	Anthony O'Neill	5/31/2018	Corrections and comments.
1.0	Dennis McDermitt	06/01/2018	Pre-publication review
1.0	Andrew Rudder	10/4/2018	Approved for Publication by: John Merto
1.1	Megan Perkins	7/15/2020	Annual Review; Minor corrections and formatting
1.2	Sean M. Hughes	11/04/2021	Annual Review

The owner of this document is the Commonwealth CISO (or designee). It is the responsibility of the document owner to maintain, update and communicate the content of this document. Questions or suggestions for improvement should be submitted to the document owner.

5.1 Annual Review

This *Glossary of Terms* document should be reviewed and updated by the document owner on an annual basis or when significant policy or procedure changes necessitate an amendment.